POLYNOMES

Dans tout le chapitre, K désignera soit $\mathbb{R}$, soit $\mathbb{C}$. On remarquera que dans les deux cas $\mathbb{R} \subset K$. On parlera de polynômes à coefficients réels ou complexes.

I - Généralités

1) Fonctions monômes

Définition : Une fonction f est une fonction monôme s'il existe un entier $n \in \mathbb{N}$ et un élément $a \in K$ tels que : $\forall x \in K \quad f(x) = ax^n$.

Si $a = 0$, alors $\forall x \in K \quad f(x) = 0$. On dira que f est le monôme nul.
Réciproquement, si $\forall x \in K \quad f(x) = 0$, alors $a = f(1) = 0$.
Si $a \neq 0$, alors on peut remarquer que a et n sont uniques. En effet, supposons que f admette deux décompositions : $\forall x \in K \quad f(x) = ax^n = bx^p$ avec a et b non nuls. Tout d'abord on remarque que $a = b = f(1)$. Si $n \neq p$, l'un d'eux est plus petit que l'autre, par exemple $p < n$. Or : $\forall x \in K \quad x^n = x^p$, donc $\forall x \in \mathbb{R} \quad x^n = x^p$, donc $\forall x \in \mathbb{R}^* \quad x^{n-p} = 1$. Or c'est impossible car $n - p > 0$, donc $2^{n-p} > 1$.

Définition : Si f est une fonction monôme non nul, il existe un unique entier $n \in \mathbb{N}$ et un unique $a \in K$ tels que : $\forall x \in K \quad f(x) = ax^n$. L'entier n est le degré du monôme et a le coefficient du monôme. Par convention, le degré du monôme nul est $-\infty$.

Notation : La fonction monôme $x \mapsto x$ est notée X, et donc $x \mapsto x^n$ est notée X^n.
Donc tout monôme non nul s'écrit de manière unique aX^n avec a et n uniques.

2) Fonctions polynômes

Définition : Une fonction P est une fonction polynôme si c'est la somme d'un nombre fini de fonctions monômes.

Si toutes les fonctions monômes sont nulles, alors $\forall x \in K \quad P(x) = 0$. On dira que P est le polynôme nul.
Sinon, comme c'est une somme finie, on désigne par n le plus haut des degrés des monômes non nuls. Donc il existe un entier $n \in \mathbb{N}$ et des coefficients réels ou complexes $(a_0, a_1, ..., a_n) \in K^{n+1}$ avec $a_n \neq 0$ tels que : $\forall x \in K \quad P(x) = \sum_{k=0}^{n} a_k x^k$.

Montrons par récurrence sur n que P ne peut pas être le polynôme nul.
Initialisation évidente pour $n = 0$.
Hérédité : On suppose, pour $n \in \mathbb{N}$, que s'il existe des coefficients $(a_0, a_1, ..., a_n) \in K^{n+1}$ avec $a_n \neq 0$ tels que : $\forall x \in K \quad P_n(x) = \sum_{k=0}^{n} a_k x^k$, alors P_n n'est pas le polynôme nul.
Montrons la propriété pour $n+1$. Soit P_{n+1} un polynôme tel qu'il existe des coefficients $(b_0, b_1, ..., b_{n+1}) \in K^{n+2}$ avec $b_{n+1} \neq 0$ vérifiant : $\forall x \in K \quad P_{n+1}(x) = \sum_{k=0}^{n+1} b_k x^k$. Montrons en raisonnant par l'absurde que P_{n+1} n'est pas le polynôme nul.
Supposons que $\forall x \in K \quad P_{n+1}(x) = 0$. Donc en particulier, $P_{n+1}(0) = 0$, donc $b_0 = 0$.

Donc $\forall x \in K \quad P_{n+1}(x) = \sum_{k=1}^{n+1} b_k x^k = xQ(x)$ avec $\forall x \in K \quad Q(x) = \sum_{k=1}^{n+1} b_k x^{k-1} = \sum_{j=1}^{n} b_{j+1} x^j$.

Or $\forall x \in K \quad xQ(x) = 0$. Donc $\forall x \in K - \{0\} \quad Q(x) = 0$ et par continuité $Q(0) = 0$.

Or $b_{n+1} \neq 0$. Donc d'après l'hypothèse de récurrence, Q n'est pas le polynôme nul.

On a donc une contradiction, donc P_{n+1} n'est pas le polynôme nul.

<u>Théorème</u> : Un polynôme est nul si et seulement si tous ses coefficients sont nuls.

La conséquence est l'unicité de l'entier *n* et des coefficients.

En effet, supposons deux décompositions : $\forall x \in K \quad P(x) = \sum_{k=0}^{n} a_k x^k = \sum_{k=0}^{p} b_k x^k$. On a donc en complétant éventuellement par des zéros : $\forall x \in K \quad \sum_{k=0}^{\mathrm{Max}(n,p)} (a_k - b_k) x^k = 0$.

C'est le polynôme nul, donc tous les coefficients sont nuls. Donc : $\forall k \in [\![0, \mathrm{Max}(n,p)]\!] \quad a_k = b_k$. Or si $n \neq p$, c'est impossible pour $k = \mathrm{Max}(n,p)$ puisque l'un est nul et pas l'autre. Donc $n = p$ et tous les coefficients sont égaux.

<u>Définition</u> : Si *P* est une fonction polynôme non nulle, il existe un unique entier $n \in \mathbb{N}$ et des coefficients uniques $(a_0, a_1, ..., a_n) \in K^{n+1}$ avec $a_n \neq 0$ tels que : $\forall x \in K \quad P(x) = \sum_{k=0}^{n} a_k x^k$. L'entier *n* est le degré du polynôme et $(a_0, a_1, ..., a_n)$ les coefficients du polynôme. Par convention, le degré du polynôme nul est $-\infty$.

On en déduit l'égalité de deux polynômes.

<u>Théorème</u> : Deux polynômes non nuls sont égaux si et seulement si ils ont le même degré et les mêmes coefficients.

<u>Notation</u> : Tout polynôme s'écrit de manière unique sous la forme $P = \sum_{k=0}^{n} a_k X^k$ ou $P(X) = \sum_{k=0}^{n} a_k X^k$ avec $a_n \neq 0$. On effectue les calculs sur les polynômes formels.

Par exemple : $(3X^2 - 5X + 4)(2X + 1) = 6X^3 - 7X^2 + 3X + 4$.

3) <u>Opérations</u>

<u>Définition</u> : On appelle $K[X]$ l'ensemble des polynômes à coefficients dans *K*.
On appelle $K_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à *n*.

On peut définir dans $K[X]$ des opérations analogues à celles des fonctions.

<u>Théorème</u> : Si $\lambda \in K$ et si *P* et *Q* appartiennent à $K[X]$, alors :

- Le produit λP est un polynôme et $\mathrm{d}°(\lambda P) = \mathrm{d}°(P)$ si $\lambda \neq 0$.
- La somme $P + Q$ est un polynôme et $\mathrm{d}°(P+Q) \leq \mathrm{Max}[\mathrm{d}°(P), \mathrm{d}°(Q)]$.
- Le produit PQ est un polynôme et $\mathrm{d}°(PQ) = \mathrm{d}°(P) + \mathrm{d}°(Q)$.
- La composée $P \circ Q$ est un polynôme et $\mathrm{d}°(P \circ Q) = \mathrm{d}°(P) \times \mathrm{d}°(Q)$.

Soient $P = \sum_{k=0}^{p} a_k X^k$ et $Q = \sum_{k=0}^{q} b_k X^k$ les deux polynômes avec $a_p \neq 0$ et $b_q \neq 0$.

- La première est évidente car $\lambda P = \sum_{k=0}^{p} \lambda a_k X^k$ et $\lambda a_p \neq 0$ car $\lambda \neq 0$ et $a_p \neq 0$.

- Soit $r = \mathrm{Max}[\mathrm{d}°(P), \mathrm{d}°(Q)]$. En ajoutant éventuellement des zéros, on peut écrire : $P+Q = \sum_{k=0}^{r} a_k X^k + \sum_{k=0}^{r} b_k X^k = \sum_{k=0}^{r} (a_k + b_k) X^k$. Donc $\mathrm{d}°(P+Q) \leq r$. Mais l'égalité n'est vraie que si $a_r + b_r \neq 0$.
- $PQ = \left(\sum_{k=0}^{p} a_k X^k\right)\left(\sum_{k=0}^{q} b_k X^k\right) = \sum_{\substack{0 \leq i \leq p \\ 0 \leq j \leq q}} a_i b_j X^{i+j}$. Le terme de plus grand haut degré correspond à $i = p$ et $j = q$. Donc $\mathrm{d}°(PQ) = p + q$ car $a_p b_q \neq 0$.
- $P \circ Q = \sum_{k=0}^{p} a_k Q^k = \sum_{k=0}^{p} a_k \left(\sum_{j=0}^{q} b_j X^j\right)^k$. Le terme de plus haut degré est obtenu pour $j = q$ dans $\left(\sum_{j=0}^{q} b_j X^j\right)^p$. C'est $a_p (b_q)^p (X^q)^p$. Donc $\mathrm{d}°(P \circ Q) = pq$ car $a_p (b_q)^p \neq 0$.

Remarque : Ces propriétés restent valables pour le polynôme nul.

II – Division euclidienne

1) Théorème fondamental

Il est à rapprocher et à distinguer de celui de la division des entiers.

Théorème : Pour tous les polynômes A et B avec $B \neq 0$ appartenant à $K[X]$, il existe un unique couple (Q, R) de polynômes appartenant à $K[X]$ tels que :

$$A = BQ + R \quad \text{avec} \quad R = 0 \text{ ou } \mathrm{d}°R < \mathrm{d}°B$$

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

Démonstration de l'existence : Si $A = 0$ ou $\mathrm{d}°A < \mathrm{d}°B$, alors $A = B \times 0 + A$, donc $(Q, R) = (0, A)$ est solution. Il reste donc le cas où $A \neq 0$ et $\mathrm{d}°A \geq \mathrm{d}°B$.

On note $B = \sum_{k=0}^{p} b_k X^k$ et on raisonne par récurrence forte sur le degré n de A ($n \geq p$).

Initialisation : Si $n = p$, alors $A = \sum_{k=0}^{p} a_k X^k$.

Donc $R = A - \frac{a_p}{b_p} B = \sum_{k=0}^{p} \left(a_k - \frac{a_p}{b_p} b_k\right) X^k$ est un polynôme nul ou de degré $q < p$ car le coefficient de rang $k = p$ est nul. Donc : $A = \frac{a_p}{b_p} B + R$ avec $R = 0$ ou $\mathrm{d}°R < \mathrm{d}°B$.

Une solution est donc (Q, R) avec $Q = \frac{a_p}{b_p}$.

Hérédité : Soit un entier $n \geq p$ tel que pour tout polynôme A avec $\mathrm{d}°A \leq n$, il existe un couple (Q, R) de polynômes tels que : $A = BQ + R$ avec $R = 0$ ou $\mathrm{d}°R < \mathrm{d}°B$.

Soit A un polynôme de degré $n+1$: $A = \sum_{k=0}^{n+1} a_k X^k$. On considère le polynôme :

$$C = A - \frac{a_{n+1}}{b_p} X^{n+1-p} B = \sum_{k=0}^{n+1} a_k X^k - \frac{a_{n+1}}{b_p} \sum_{k=0}^{p} b_k X^{n+1-p+k} = \sum_{k=0}^{n+1} a_k X^k - \frac{a_{n+1}}{b_p} \sum_{j=n+1-p}^{n+1} b_{j-n-1+p} X^j$$

C'est un polynôme nul ou de degré inférieur ou égal à $n+1$ dont le coefficient du terme de rang $n+1$ est $a_{n+1} - \frac{a_{n+1}}{b_p} b_p = 0$. Donc $C = 0$ ou $\mathrm{d}°C \leq n$.

Donc il existe un couple (Q_1, R_1) de polynômes tels que : $C = BQ_1 + R_1$ avec $R_1 = 0$ ou $d°R_1 < d°B$. Donc $A = \dfrac{a_{n+1}}{b_p} X^{n+1-p} B + C = B\left(\dfrac{a_{n+1}}{b_p} X^{n+1-p} + Q_1\right) + R_1$.

Cela prouve l'existence du couple (Q, R) lorsque $d°A = n+1$.

<u>Conclusion</u> : L'existence du couple (Q, R) est démontrée pour tout entier $n \geq p$.

<u>Démonstration de l'unicité</u> : On suppose qu'il existe deux couples solutions :

$A = BQ_1 + R_1 = BQ_2 + R_2$ avec $\begin{cases} R_1 = 0 \text{ ou } d°R_1 < d°B \\ R_2 = 0 \text{ ou } d°R_2 < d°B \end{cases}$. Donc $B(Q_1 - Q_2) = R_2 - R_1$.

Or si $Q_1 \neq Q_2$, ce qui implique $R_1 \neq R_2$, alors $d°B(Q_1 - Q_2) = d°B + d°(Q_1 - Q_2)$, donc $d°B(Q_1 - Q_2) \geq d°B$, ce qui est impossible car $d°(R_2 - R_1) < d°B$.

Donc $Q_1 = Q_2$, ce qui implique $R_1 = R_2$. L'unicité est démontrée.

2) Calcul pratique

On dispose les calculs comme pour diviser des entiers.

<u>Exemple 1</u> : Division de $A = 3X^3 + 4X^2 - 2X - 5$ par $B = X + 1$

$$\begin{array}{r|l} 3X^3 + 4X^2 - 2X - 5 & X + 1 \\ \cline{2-2} \underline{3X^3 + 3X^2} \qquad\qquad & 3X^2 + X - 3 \\ X^2 - 2X - 5 & \\ \underline{X^2 + X} \qquad & \\ -3X - 5 & \\ \underline{-3X - 3} & \\ -2 & \end{array}$$

Le quotient est $Q = 3X^2 + X - 3$ et le reste est $R = -2$.

Donc $3X^3 + 4X^2 - 2X - 5 = (X+1)(3X^2 + X - 3) - 2$.

<u>Exemple 2</u> : Division de $A = X^3 - 5X^2 + 3X - 1$ par $B = X^2 - X + 1$

$$\begin{array}{r|l} X^3 - 5X^2 + 3X - 1 & X^2 - X + 1 \\ \cline{2-2} \underline{X^3 - X^2 + X} \qquad & X - 4 \\ -4X^2 + 2X - 1 & \\ \underline{-4X^2 + 4X - 4} & \\ -2X + 3 & \end{array}$$

Le quotient est $Q = X - 4$ et le reste est $R = -2X + 3$.

Donc $X^3 - 5X^2 + 3X - 1 = (X^2 - X + 1)(X - 4) - 2X + 3$.

<u>Exemple 3</u> : Division de $A = 2X^3 - 5X^2 + X + 2$ par $B = X - 1$

$$\begin{array}{r|l} 2X^3 - 5X^2 + X + 2 & X - 1 \\ \cline{2-2} \underline{2X^3 - 2X^2} \qquad\qquad & 2X^2 - 3X - 2 \\ -3X^2 + X + 2 & \\ \underline{-3X^2 + 3X} \qquad & \\ -2X + 2 & \\ \underline{-2X + 2} & \\ 0 & \end{array}$$

Le quotient est $Q = 2X^2 - 3X - 2$ et le reste est $R = 0$.

Donc $2X^3 - 5X^2 + X + 2 = (X-1)(2X^2 - 3X - 2)$.

3) Multiples et diviseurs

> Définition : Un polynôme $B \neq 0$ est un diviseur d'un polynôme A, ce qui équivaut à dire que A est multiple de B, si le reste de la division euclidienne de A par B est $R = 0$.

On dit que A est divisible ou factorisable par B : $\exists Q \in K[X] \quad A = BQ$.

> Définition : Un polynôme est irréductible s'il n'admet pas de diviseurs de degré supérieur ou égal à 1.

Attention : Le polynôme $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$, mais pas dans $\mathbb{C}[X]$ puisque : $X^2 + 1 = (X - i)(X + i)$.

4) Cas particulier

Soit $\alpha \in K$, P un polynôme de $K[X]$ et $B = X - \alpha$.

Dans la division euclidienne de P par B, il existe un unique couple (Q, R) de polynômes tels que : $P = (X - \alpha)Q + R$ avec $R = 0$ ou $d°R < 1$. Donc R est un polynôme constant (nul ou pas) : $R = r$.

Donc $\forall x \in K \quad P(x) = (x - \alpha)Q(x) + r$. Donc $P(\alpha) = r$.

> Théorème : Pour tout $\alpha \in K$ et tout polynôme $P \in K[X]$, il existe un unique polynôme $Q \in K[X]$ tel que $P = (X - \alpha)Q + P(\alpha)$.

La division euclidienne peut être utilisée pour calculer $P(\alpha)$.

Dans le cas de la division par $(X - \alpha)$, on peut adopter une autre disposition.

Exemple : Division de $P = 3X^5 - 4X^4 + X^2 - 5X + 2$ par $(X - 2)$.

$$
\begin{array}{r|l}
3X^5 - 4X^4 \qquad + X^2 - 5X + 2 & X - 2 \\
\underline{3X^5 - 6X^4} \qquad\qquad\qquad\quad & 3X^4 + 2X^3 + 4X^2 + 9X + 13 \\
2X^4 \qquad + X^2 - 5X + 2 & \\
\underline{2X^4 - 4X^3} \qquad\qquad\quad & \\
4X^3 + X^2 - 5X + 2 & \\
\underline{4X^3 - 8X^2} \qquad\quad & \\
9X^2 - 5X + 2 & \\
\underline{9X^2 - 18X} \quad & \\
13X + 2 & \\
\underline{13X - 26} & \\
28 &
\end{array}
$$

Donc : $3X^5 - 4X^4 + X^2 - 5X + 2 = (X - 2)(3X^4 + 2X^3 + 4X^2 + 9X + 13) + 28$.

Méthode de Hörner :

Dans la première ligne, on copie les coefficients a_k de P sans oublier les zéros.

Dans la deuxième ligne, on calcule les coefficients b_k de Q. Si $d°P = n$, alors $d°Q = n - 1$. Il y a donc une case inutilisée à droite qui contiendra $P(\alpha)$.

a_n	a_{n-1}	a_{n-2}	$\cdots$	a_2	a_1	a_0
b_{n-1}	b_{n-2}	b_{n-3}	$\cdots$	b_1	b_0	$P(\alpha)$

On a pour premier coefficient : $b_{n-1} = a_n$.

Ensuite, les autres coefficients sont calculés de proche en proche : $b_k = a_{k+1} + \alpha b_{k+1}$.

C'est le calcul effectué dans la division euclidienne schématisé par :

	a_{k+1}
b_{k+1}	b_k

La dernière case est remplie par : $P(\alpha) = a_0 + \alpha b_0$.
Dans l'exemple $\alpha = 2$, donc pour tout k : $b_k = a_{k+1} + 2b_{k+1}$

3	-4	0	1	-5	2
3	2	4	9	13	***28***

Donc : $3X^5 - 4X^4 + X^2 - 5X + 2 = (X-2)(3X^4 + 2X^3 + 4X^2 + 9X + 13) + 28$.
Mais cette méthode ne fonctionne que pour la division par $(X - \alpha)$.

III – Racines

1) Définition et caractérisation

Définition : Un élément α de K est racine d'un polynôme P si $P(\alpha) = 0$.

Or on a vu que : $\forall \alpha \in K \quad P = (X - \alpha)Q + P(\alpha)$.
On en déduit la caractérisation suivante :

Théorème : Un élément α de K est racine d'un polynôme P si et seulement si P est divisible par $(X - \alpha)$.

On utilise en général ce théorème pour factoriser un polynôme.
Si P possède deux racines distinctes α_1 et α_2, alors P est divisible par $(X - \alpha_1)$: $P = (X - \alpha_1)Q_1$ et $P(\alpha_2) = (\alpha_2 - \alpha_1)Q_1(\alpha_2) = 0$, donc $Q_1(\alpha_2) = 0$, donc α_2 est racine de Q_1, donc Q_1 est divisible par $(X - \alpha_2)$. Donc : $P = (X - \alpha_1)(X - \alpha_2)Q_2$.

Conséquence : Un polynôme de degré n possède au plus n racines distinctes.

2) Ordre de multiplicité d'une racine

Il peut arriver que α soit racine de P, donc que $P = (X - \alpha)Q$ avec $Q(\alpha) = 0$, ce qui entraîne $Q = (X - \alpha)R$, et donc $P = (X - \alpha)^2 R$.

Exemple : $P = X^3 + X^2 - 5X + 3 = (X-1)(X^2 + 2X - 3) = (X-1)^2(X+3)$.

Définition : On appelle ordre de multiplicité d'une racine α d'un polynôme P le plus grand entier m tel que P soit divisible par $(X - \alpha)^m$.

Cela revient à dire que $P = (X - \alpha)^m Q$ avec $Q(\alpha) \neq 0$. On peut remarquer que :
$P' = m(X-\alpha)^{m-1}Q + (X-\alpha)^m Q' = (X-\alpha)^{m-1}[mQ + (X-\alpha)Q'] = (X-\alpha)^{m-1}Q_1$
avec $Q_1(\alpha) = mQ(\alpha)$, donc $Q_1(\alpha) \neq 0$. Donc α est racine d'ordre $m-1$ de $P' = P^{(1)}$.
On peut donc recommencer : α est racine d'ordre $m-2$ de $P'' = P^{(2)}$, racine d'ordre $m-3$ de $P^{(3)}$, …, racine d'ordre 1 de $P^{(m-1)}$, mais pas racine de $P^{(m)}$.
Réciproquement, supposons que α soit racine de P, de $P' = P^{(1)}$, de $P'' = P^{(2)}$, …, de $P^{(m-1)}$, mais pas racine de $P^{(m)}$. Si on effectue la division de P par $(X - \alpha)^m$, on obtient : $P = (X - \alpha)^m Q + R$ avec $d°R < m$.
Donc en dérivant k fois : $\forall k \in [\![0, m-1]\!] \quad P^{(k)} = [(X - \alpha)^m Q]^{(k)} + R^{(k)}$.
Or d'après l'étude précédente : $\forall k \in [\![0, m-1]\!] \quad [(X - \alpha)^m Q]^{(k)}(\alpha) = 0$
donc avec l'hypothèse : $\forall k \in [\![0, m-1]\!] \quad R^{(k)}(\alpha) = 0$.
Or $R^{(k)}$ est un polynôme dont le degré est $d°R - k$.
Donc $R^{(m-1)}$ est constant. Or $R^{(m-1)}(\alpha) = 0$. Donc $R^{(m-1)} = 0$.
Donc $R^{(m-2)}$ est constant et $R^{(m-2)}(\alpha) = 0$. Donc $R^{(m-2)} = 0$…

Et ainsi de suite, jusqu'à $R = 0$. Donc $P = (X - \alpha)^m Q$ et α est racine d'ordre m.

<u>Théorème</u> : Un élément α de K est racine d'ordre m d'un polynôme P si et seulement si $\forall k \in [\![0, m-1]\!]\quad P^{(k)}(\alpha) = 0$ et $P^{(m)}(\alpha) \neq 0$.

3) Factorisation dans le corps des complexes

On a vu que dans $\mathbb{R}$, tout polynôme ne possède pas forcément une racine, par exemple le polynôme $X^2 + 1$. Par contre :

<u>Théorème de D'Alembert-Gauss</u> : Tout polynôme non constant à coefficients réels ou complexes possède au moins une racine dans $\mathbb{C}$.

Ce théorème est admis. Il est faux dans $\mathbb{R}$ (exemple : $X^2 + 1$).

<u>Conséquence</u> : Dans $\mathbb{C}[X]$, les seuls polynômes (non constants) irréductibles sont les polynômes de degré 1.

Soit $P \in \mathbb{C}[X]$. Le polynôme P, s'il n'est pas constant, possède au moins une racine α_1 dans $\mathbb{C}$, donc est divisible par $(X - \alpha_1)$: $P = (X - \alpha_1)Q_1$ avec $d°Q_1 = n - 1$.
Si $n \geq 2$, Q_1 n'est pas constant, donc possède au moins une racine α_2 dans $\mathbb{C}$, donc est divisible par $(X - \alpha_2)$: $Q_1 = (X - \alpha_2)Q_2$ avec $d°Q_2 = n - 2$. Donc le polynôme P s'écrit $P = (X - \alpha_1)(X - \alpha_2)Q_2$ … et ainsi de suite jusqu'à obtenir un polynôme constant, ce qui arrivera au bout de n factorisations.

Donc le polynôme P s'écrit : $P = a(X - \alpha_1)(X - \alpha_2)....(X - \alpha_n) = a\prod_{i=1}^{n}(X - \alpha_i)$.

Les racines α_1, α_2, …, α_n ne sont pas forcément distinctes.

<u>Théorème</u> : Tout polynôme P non constant à coefficients réels ou complexes qui possède k racines distinctes α_1, α_2, …, α_k dans $\mathbb{C}$ s'écrit : $P = a\prod_{i=1}^{k}(X - \alpha_i)^{m_i}$ où m_i est l'ordre de multiplicité de la racine α_i et a le coefficient dominant de P.

4) Factorisation dans le corps des réels

Soit $P \in \mathbb{R}[X]$. Donc $P = \sum_{k=0}^{n} a_k X^k$ avec tous les a_k réels : $\forall x \in \mathbb{R}\quad P(x) = \sum_{k=0}^{n} a_k x^k$.

Comme $\mathbb{R} \subset \mathbb{C}$, on considère le polynôme dans $\mathbb{C}[X]$: $\forall z \in \mathbb{C}\quad P(z) = \sum_{k=0}^{n} a_k z^k$.

On peut remarquer que : $\forall z \in \mathbb{C}\quad \overline{P(z)} = \sum_{k=0}^{n} a_k \overline{z^k} = \sum_{k=0}^{n} a_k \overline{z}^k = P(\overline{z})$.

Donc si α est une racine de P dans $\mathbb{C}$, alors $P(\alpha) = 0$, et donc $P(\overline{\alpha}) = 0$.
Donc si α est racine de P dans $\mathbb{C}$, alors $\overline{\alpha}$ est aussi racine de P dans $\mathbb{C}$. Elles peuvent être distinctes ou confondues. Si $\alpha = \overline{\alpha}$, alors la racine α est réelle.

<u>Théorème</u> : Les racines d'un polynôme P non constant à coefficients réels sont soit réelles, soit complexes conjuguées deux à deux (avec le même ordre de multiplicité).

Dans la factorisation de P, on a donc :

- soit des facteurs de la forme $(X - \alpha)^m$ avec α réel.
- soit des facteurs de la forme $[(X - \alpha)(X - \overline{\alpha})]^m = [X^2 - (\alpha + \overline{\alpha})X + \alpha\overline{\alpha}]^m$ où $X^2 - (\alpha + \overline{\alpha})X + \alpha\overline{\alpha}$ est un polynôme irréductible dans $\mathbb{R}$.

<u>Conséquence</u> : Dans $\mathbb{R}[X]$, les seuls polynômes (non constants) irréductibles sont les polynômes de degré 1 et les polynômes de degré 2 avec un discriminant négatif.

On passe souvent par $\mathbb{C}$ pour factoriser un polynôme dans $\mathbb{R}$.

<u>Exemple</u> : Factoriser dans $\mathbb{R}$ le polynôme $P = X^4 + 1$.

Les racines de $P = X^4 + 1$ dans $\mathbb{C}$ sont les racines $4^{\text{ièmes}}$ de $-1 = e^{i\pi}$.

Les racines sont donc $\alpha_k = e^{\frac{(2k+1)i\pi}{4}}$ pour $k \in [\![0,3]\!]$. On obtient : $\alpha_0 = e^{\frac{i\pi}{4}} = \frac{\sqrt{2}}{2}(1+i)$,

$\alpha_1 = i\alpha_0 = \frac{\sqrt{2}}{2}(-1+i)$, $\alpha_2 = -\alpha_0 = \frac{\sqrt{2}}{2}(-1-i)$ et $\alpha_3 = -i\alpha_0 = \frac{\sqrt{2}}{2}(1-i)$.

Donc : $P = \left(X - \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right)\left(X + \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right)\left(X + \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)\left(X - \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)$.

$$P = \left[\left(X - \frac{\sqrt{2}}{2}\right)^2 - \left(i\frac{\sqrt{2}}{2}\right)^2\right]\left[\left(X + \frac{\sqrt{2}}{2}\right)^2 - \left(i\frac{\sqrt{2}}{2}\right)^2\right] = (X^2 - X\sqrt{2} + 1)(X^2 + X\sqrt{2} + 1)$$

On obtient la factorisation de P en produit de deux polynômes irréductibles sur $\mathbb{R}$.

<u>Autre méthode</u> : $P = X^4 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 - X\sqrt{2} + 1)(X^2 + X\sqrt{2} + 1)$.